BEST AVAILABLE COPY

(72) Inventors: OULD-BRAHIM, Hamid; 21 Wynridge Place, Kanata, Ontario K2M 2S8 (CA). FEDYK, Donald; 220 Hayden Road, Groton, MA 01450 (US).

*[Continued on next page]*

(54) Title: RESOURCE ALLOCATION USING AN AUTO-DISCOVERY MECHANISM FOR PROVIDER-PROVISIONED LAYER-2 AND LAYER-3 VIRTUAL PRIVATE NETWORKS
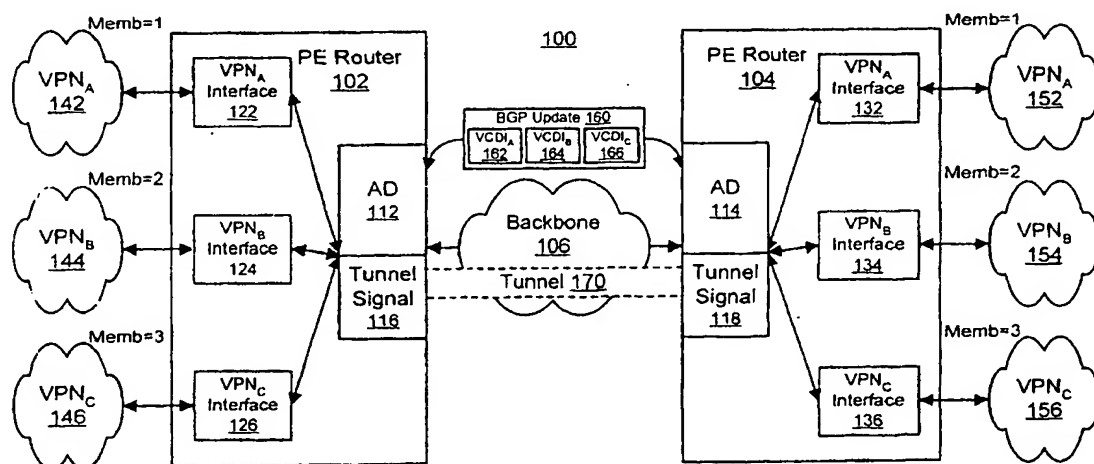
(57) Abstract: A technique for resource distribution using an auto-discovery mechanism for Provider-Provisioned Layer-2 and Layer-3 Virtual Private Networks. In one particular exemplary embodiment, the technique may be realized by a method for establishing a Virtual Private Network (VPN) tunnel between a first provider edge (PE) device and a second (PE) device of a provider-provisioned VPN. The method may comprise advertising at least one tunnel-based parameter to one or more PE devices over a network backbone using an auto-discovery mechanism, the one or more PE devices including at least one of the first and second PE devices. The method further may comprise configuring a VPN tunnel between the first and second PE devices based at least in part on the at least one tunnel-based parameter.

RESOURCE ALLOCATION USING AN AUTO-DISCOVERY MECHANISM FOR PROVIDER-PROVISIONED LAYER-2 AND LAYER-3 VIRTUAL PRIVATE NETWORKS

FIELD OF THE INVENTION

5   The present invention relates generally to Virtual Private Networks (VPNs) and, more particularly, to a technique for implementing resource allocation for implementing VPN services using an auto-discovery process for configuring one or more Layer-2 and Layer-3 VPNs.

BACKGROUND OF THE INVENTION

10

In the absence of a privacy mechanism, sensitive data (e.g., passwords, account numbers, proprietary information, etc.) transmitted over a network may be susceptible to interception by unauthorized parties. One

15   privacy mechanism commonly used to protect network data is the Virtual Private Network (VPN). Using specialized tunneling protocols and optionally secure encryption techniques, data integrity and privacy may be maintained in a VPN in what seems like a dedicated point-to-point connection.

20   Network-based VPNs typically are implemented through a tunneling mechanism. In general, the tunneling mechanism encapsulates the packet headers and/or payload prior to transmission of the packet over an established VPN tunnel. As a result, the transmission of a VPN-based packet only uses

25   non-tunneling information, such as the Internet Protocol (IP) addresses of the ends of the tunnels, while the sensitive information, such as the source and destination IP addresses and sensitive payload data, remains encapsulated. Exemplary tunneling mechanisms include IP/IP tunneling, Generic Router

30   Encapsulation (GRE) tunneling, IP Security (IPSec) tunneling

and Multi-Protocol Label Switching (MPLS) tunneling. The
configuration of VPN tunnel typically is specific to the
particular type of VPN used.

        A typical Network IP-based VPN generally includes at
5   least two provider edge (PE) devices (e.g., a VPN-enabled
router) interconnected via a series of provider devices (e.g.,
routers) that form a network backbone, where the network
backbone typically includes one or more public networks, such
as, for example, the Internet or a wide area network (WAN).
10 Connected to each PE device are one or more customer edge (CE)
devices, such as a workstation or personal computer. In this
type of network-based VPN, VPN tunnels are established between
PE devices, rather than between CE devices. These tunnels,
herein referred to as PE-PE tunnels, typically are established
15 at either Layer-2 or Layer-3 of the International Standard
Organization's Open System Interconnect (ISO/OSI) network
model. Exemplary VPN mechanisms at Layer-2 include Virtual
Private LAN Service (VPLS)(see Waldemar Augustyn et al.,
"Requirements for Virtual Private LAN Services (VPLS),"
20 October 2002, available at <http://www.ietf.org/internet-
drafts/draft-ietf-ppvpn-vpls-requirements-01.txt>, the
entirety of which is hereby incorporated herein by reference)
and Virtual Private Wire (VPW)(see Eric Rosen et al., "L2VPN
Framework," February 2003, available at
25 <http://www.ietf.org/internet-drafts/draft-ietf-ppvpn-l2-
framework-03.txt>, the entirety of which is hereby
incorporated herein by reference). Exemplary VPN mechanisms
at Layer-3 include Virtual Routing (VR)-based mechanisms, such
as VR using Border Gateway Protocol (BGP)(see Hamid Ould-
30 Brahim et al. "Network based IP VPN Architecture using Virtual
Routers," July 2002, available at
<http://www.ietf.org/internet-drafts/draft-ietf-ppvpn-vpn-vr-

03.txt>, the entirety of which is hereby incorporated herein
by reference) or VPNs based on RFC 2547bis (often referred to
as BGP/MLPS-based VPNs)(see Eric Rosen et al., "BGP/MPLS VPNs"
available at <http://www.ietf.org/internet-drafts/draft-ietf-
5   ppvpn-rfc2547bis-03.txt>, October 2002, the entirety of which
is hereby incorporated herein by reference).

        Regardless of the VPN mechanism used, a primary step
in establishing a network-based VPN is to provide information
about each VPN configured on a local PE device to the
10 remaining remote PE devices. A number of mechanisms may be
implemented to achieve this distribution of PE information,
such as BGP, Domain Name Service (DNS), Remote Authentication
Dial In User Service (RADIUS), and the like. Such mechanisms
are well known in the art. After distributing this PE
15 information, one or more PE-PE tunnels typically are
established based in part on information received through a
VPN auto-discovery mechanism.

        Various tunnel signalling protocols may be used to
establish and maintain VPN tunnels, such as, for example,
20 Resource Reservation Protocol (RSVP), Resource Reservation
Protocol - Traffic Engineered (RSVP-TE), Label Distribution
Protocol (LDP), Constraint-based Routing LDP (CR-LDP),
Asynchronous Transfer Mode (ATM), Frame Relay, Generic Routing
Encapsulation (GRE), IPSec, and the like.

25   Various parameters for VPN tunnels in conventional
Layer-2 and Layer-3 VPNs typically are configured manually by
the service provider. As a result, the scalability of such
conventional VPN implementations is limited due to the
difficulty in manually configuring a complex and dynamic VPN
30 system having a large number of PE devices and/or constantly
changing system requirements, such as a continuous changing

3

number of tunnels/VPNs, constant, continuous changes in
resources such as bandwidth, delay and/or Quality of Service
(QoS) requirements, and the like. Further, these conventional
VPN implementations generally lack a defined mechanism to
5 relate VPN tunnels to a per VPN or per set of VPNs resources
such as QoS profiles or other tunnel-specific parameters. As
a result, the flexibility of such conventional VPN systems is
compromised because the VPN is unable to predictably respond
to changes in bandwidth requirements, QoS requirements, and
10 the like.

In view of the foregoing, it would be desirable to
provide a technique for facilitating the configuration of VPN
tunnels based at least in part on supplied parameters in an
auto-discovery manner. More particularly, it would be
15 desirable to implement resource profiles such as Quality of
Service (QoS) parameters using a VPN auto-discovery as an
extension to existing auto-discovery mechanisms in an
efficient and cost effective manner.

SUMMARY OF THE INVENTION

20 In accordance with one embodiment of the present
invention, a method for establishing a Virtual Private Network
(VPN) tunnel between a first provider edge (PE) device and a
second (PE) device of a Provider-Provisioned VPN (PPVPN) is
provided. The method comprises advertising at least one
25 tunnel-based parameter to one or more PE devices over a
network backbone using an auto-discovery mechanism, the one or
more PE devices including at least one of the first and second
PE devices and configuring a VPN tunnel between the first and
second PE devices based at least in part on the at least one
30 tunnel-based parameter. A computer signal embodied in a
carrier wave readable by a computing system and encoding a

4

computer program of instructions for executing a computer
process may be used to perform the above method.

In a Provider-Provisioned Virtual Private Network
(PPVPN), a system is provided in accordance with another
5   embodiment of the present invention. The system comprises
auto-discovery means for distributing at least one Virtual
Private Network (VPN) tunnel-based parameter to at least a
first and second provider edge (PE) devices and tunnel
signalling means for configuring a VPN tunnel over a network
10   backbone between the first and second PE devices based at
least in part on the at least one tunnel-based parameter.

In a distributed network, a Provider-Provisioned
Virtual Private Network (PPVPN) system is provided in
accordance with yet another embodiment of the present
15   invention. The system comprises a network backbone, a first
and second provider edge (PE)device, each operably connected
to the network backbone and an auto-discovery mechanism for
distributing at least one VPN tunnel parameter to at least the
first and second PE devices as an extension to an auto-
20   discovery protocol.

The present invention will now be described in more
detail with reference to exemplary embodiments thereof as
shown in the appended drawings. While the present invention
is described below with reference to preferred embodiments, it
25   should be understood that the present invention is not limited
thereto. Those of ordinary skill in the art having access to
the teachings herein will recognize additional
implementations, modifications, and embodiments, as well as
other fields of use, which are within the scope of the present
30   invention as disclosed and claimed herein, and with respect to
which the present invention could be of significant utility.

5

BRIEF DESCRIPTION OF THE DRAWINGS

In order to facilitate a fuller understanding of the present invention, reference is now made to the appended drawings. These drawings should not be construed as limiting the present invention, but are intended to be exemplary only.

Figure 1 is a schematic diagram illustrating a Provider-Provisioned Virtual Private Network (PPVPN) system utilizing a VPN auto-discovery mechanism in accordance with at least one embodiment of the present invention.

Figure 2 is a flow diagram illustrating an overview of a VPN auto-discovery mechanism for establishing and/or maintaining a provider-edge-to-provider-edge (PE-PE) tunnel in accordance with at least one embodiment of the present invention.

Figure 3 is a flow diagram illustrating an exemplary implementation of the VPN auto-discovery mechanism of Figure 2 in a RFC 2547bis-based VPN in accordance with at least one embodiment of the present invention.

Figure 4 is a flow diagram illustrating an exemplary implementation of the VPN auto-discovery mechanism of Figure 2 in a Virtual Routing-based VPN in accordance with at least one embodiment of the present invention.

Figure 5 is a flow diagram illustrating an exemplary implementation of the VPN auto-discovery mechanism of Figure 2 in a Layer-2 VPN using a Virtual Private Local Area Network Service (VPLS)-based or VPW-based mechanism in accordance with at least one embodiment of the present invention.

DETAILED DESCRIPTION OF EXEMPLARY EMBODIMENT(S)

Figures 1-5 illustrate various exemplary implementations for creating scalable VPN PE-PE tunnels in Level-2 or Level-2 PPVPNs using an auto-discovery mechanism.
5 Information regarding the establishment and/or configuration of a tunnel between two PE devices may be advertised among the PE devices of a network. This information may include, for example, the desired tunnel signalling protocol, the Quality of Service (QoS) profile for the tunnel, the PE tunnel
10 endpoint, membership information, the VPN technology to be used, etc. In at least one embodiment, this information may be advertised as an extension to a conventional auto-discovery mechanism commonly used in VPNs, such as the Border Gateway Protocol (BGP), directory service protocols (e.g., Domain Name
15 Service (DNS), RADIUS), and the like. After distributing this information, a tunnel may be established between the appropriate PE devices based at least in part on the supplied information. Alternatively, the PEs may select an existing tunnel that complies with some or all of the supplied
20 parameters. By implementing an auto-discovery technique to distribute the QoS profile for the purpose of VPN tunnel configuration and/or establishment information, the scalability of the VPN system may be enhanced because the QoS profile of a tunnel may be set according to the requirements
25 of the VPN services, where the information is distributed among the PEs in an automated fashion rather than implemented by manual configuration as conventional VPN systems.

Referring now to Figure 1, an exemplary PPVPN system 100 implementing a capability discovery mechanism is
30 illustrated in accordance with at least one embodiment of the present invention. In the illustrated example, the PPVPN

7

system 100 includes PE routers 102, 104 connected via a
network backbone 106. Although described herein as VPN-
enabled routers, the PE routers 102, 104 may include other
appropriate PE devices such as, for example, MPLS/IP Layer-2

5   switches. The network backbone 106 may include any number of
provider network devices interconnected using one or more data
link types such as, for example, IP, ATM, Frame Relay (FR),
Time Division Multiplexing (TDM), Ethernet, Optical Ethernet,
and the like.

10   Connected to each PE router 102, 104 is one or more
VPN segments, such as VPN segments 142-146 connected to PE
router 102 and VPN segments 152-156 connected to PE router
104. Each VPN segment 142-146, 152-156 may include one or
more networked customer edge (CE) devices as well as devices

15   to facilitate network connectivity, such as hubs, routers,
switches, bridges, and the like. As understood in the art, CE
devices may include any of a variety of networked devices,
such as personal computers, laptops, workstations, and the
like.

20   In general, each VPN segment connected to the PE
router 102 is a member of the same VPN as a VPN segment
connected to the PE Router 104, thereby allowing a VPN to be
established between devices on the VPN segments. In the
illustrated example, the VPN segments 142, 152 are members of

25   VPN_A, the VPN segments 144, 154 are members of VPN_B, and the
VPN segments 146, 156 are members of VPN_C. Although each VPN
segment is illustrated in Figure 1 as a member of a single
VPN, it will be appreciated that a VPN segment may be a member
of a plurality of VPNs. Likewise, a CE device may be a member

30   of a plurality of VPNs and therefore may be a member of more
than one VPN segment.

8

To facilitate communications between VPN segments, each PE router 102, 104 may include a VPN interface corresponding to a VPN segment. To illustrate, the PE router 102 may include VPN interfaces 122-126 to interface with VPN

5 segments 142-146, respectively, and the PE router 104 may include VPN interfaces 132-136 to interface with VPN segments 152-156, respectively.

Depending on the VPN technology utilized, the VPN interfaces 122-126, 132-136 may be implemented in any of a

10 variety of ways. For example, if the PPVPN system 100 implements a Layer-3 VPN using Virtual Routing (VR), the VPN interfaces 122-126, 132-136 may include Virtual Routers implemented by the PE routers 102, 104 to provide Virtual Routing between the CE devices on the VPN segments. Virtual

15 Routing and Virtual Routers are well known to those skilled in the art.

For example, if the PPVPN system 100 implements a Layer-3 VPN using RFC2547bis, the VPN interfaces 122-126, 132-136 may include Virtual Routing and Forwarding (VRF)

20 implemented by the PE routers 102, 104 to provide Virtual Routing and Forwarding tables between the CE devices on the VPN segments. RFC2547bis and Virtual Routing and Forwarding are well known to those skilled in the art.

Alternatively, if the PPVPN system 100 implements a

25 Layer-2 VPW in accordance with VPW (see, e.g., "L2VPN Framework," supra), the VPN interfaces 122-126, 132-136 may include a Virtual Switching Instance (VSI) implemented by the PE routers 102, 104 to provide Layer-2 attachment circuits between the CE devices on the VPN segments. Layer-2 VPNs and

30 Virtual Switching Instances are well known to those skilled in the art.

9

Further, in at least one embodiment, the PE router 102 may include an auto-discovery (AD) component 112 and a tunnel signalling component 116 and the PE route 104 may include an AD component 114 and a tunnel signalling component
5   118.   As discussed in greater detail below, the tunnel signalling components 116, 118 may be adapted to create, configure and/or maintain one or more VPN tunnels 170 between the PE routers 102-104 using one or more tunnel signalling mechanisms.   Exemplary tunnel signalling mechanisms
10 implemented by the tunnel signalling components 116, 118 may include, for example, RSVP, RSVP-TE, LDP, CR-LDP, and the like.

A number of supplied parameters may be used by the tunnel signalling components 116, 118 to create, configure
15 and/or maintain the one or more tunnels 170 between the PE router 102 and the PE router 104.   These parameters may include, for example: the type of tunnelling mechanism to be used (i.e., specifying RSVP-TE or CR-LDP); the QoS profile for each tunnel 170; the PE tunnel endpoints for a particular VPN
20 membership; the VPN technology to use (e.g., Layer-3 technology v. Layer-2 technology, 2547bis v. Virtual Routing, etc.); and the like.   For ease of discussion, this information is collectively referred to herein as VPN Capability Discovery Information (VCDI).

25   In conventional PPVPN systems, this information typically is configured manually at each PE router for each VPN membership.   In one embodiment, however, the AD component 112 may be adapted to advertise this information to other PE routers on the backbone 106 using an auto-discovery mechanism
30 (described in greater detail below).   The AD component 112 then may provide received VCDI information to the tunnel

10

signalling component 116 for use in creating, maintaining,
and/or configuring the one or more tunnels 170 associated with
the VCDI information.

5   The auto-discovery mechanism may be implemented in
any of a variety of ways. In at least one embodiment, the
auto-discovery mechanism may be implemented as an extension to
conventional information distribution protocols, such as BGP,
DNS, and RADIUS. To illustrate using BGP, the VCDI
information for each of VPN_A, VPN_B, and VPN_C, may be determined
10 and transmitted to the PE routers 102, 104 as profiles 162-
166, respectively, as part of a BGP UPDATE 160 transmitted
over the backbone 106. Upon receipt of the BGP UPDATE 160,
the AD components 112, 114 (each BGP-enabled in this case)
then may extract the profiles 162-166 and supply the VCDI
15 information of the profiles 162-166 to the tunnel signalling
components 116, 118 for use in creating, maintaining, and/or
configuring the VPN tunnel(s) 170 associated with each VPN.
DNS, RADIUS, and other directory service protocols may be
extended in a similar manner to distribute VCDI to the PE
20 routers. Accordingly, rather than having to manually
configure VPN tunnels at each PE router, the VPN tunnel
configuration information (i.e., the VCDI) may be "piggy-
backed" onto auto-discovery information by extending the auto-
discovery protocol to include the transmission of the VCDI
25 information.

           Referring now to Figure 2, an exemplary overview of
the VPN tunnel configuration process is illustrated in
accordance with at least one embodiment of the present
invention. In the illustrated example, the VPN tunnel
30 configuration process 200 initiates at step 202, wherein the
VCDI information for a given VPN may be determined. The VCDI

information may include information regarding the
configuration of one or more VPN tunnels between PE routers
for the VPN. For example, the VCDI information may specify
the PE tunnel endpoints, community route targets, resource

5   parameters (e.g., minimum bandwidth, maximum delay, committed
burst size, committed rate, jitter, error, ownership, physical
position, type of transport medium, etc.), topology
information, and other parameters utilized by the tunnel
signalling mechanisms to establish and/or configure a VPN

10 tunnel.

At step 204, the VCDI information obtained at step
202 may be advertised to some or all of the PE routers on the
backbone. The advertisement of the VCDI information, in one
embodiment, includes incorporating the VCDI information into a

15 conventional information distribution protocol. For example,
the VCDI information could be incorporated as an extension of
BGP and transmitted between PE routers using, for example, a
BGP UPDATE transmission. Alternatively, the VCDI information
could be formatted and transmitted in accordance with DNS or

20 RADIUS. Multicast-based protocols also may be extended to
multicast the VCDI information to some or all of the PE
routers over the backbone.

At step 206, upon receipt of the VCDI information, a
PE router may begin negotiating the creation of a VPN (or per

25 VPN) PE-PE tunnel based at least in part on the received VCDI
information. As noted above, the creation and configuration
of a VPN tunnel is well known in the art (see Hamid Ould-
Brahim et al., "Using BGP as an Auto-Discovery Mechanism for
Network-Based VPNs," August 2002, available at

30 <http://www.ietf.org/internet-drafts/draft-ietf-ppvpn-bgvpn-
auto-03.txt>, the entirety of which is hereby incorporated

12

herein by reference). In creating and configuring the VPN
tunnel from the VCDI information, any of a variety of
tunnelling mechanisms may be used, as appropriate. Examples
of such mechanisms include, for example, RSVP-TE, LDP, CR-LDP,
5   and the like. After creating the VPN tunnel, CE devices on
the various VPN segments them may utilize the VPN tunnel to
transmit data securely between VPN segments.

Referring now to Figures 3-5, various exemplary
implementations of the process 200 of Figure 2 for certain VPN
10 technologies are illustrated in accordance with at least one
embodiment of the present invention. Figure 3 illustrates an
exemplary implementation of the process 200 for a VPN system
implementing a Layer-3 VPN using RFC 2547bis. Figure 4
illustrates an exemplary implementation of the process 200 for
15 a VPN system implementing a Layer-3 VPN using Virtual Routing.
Figure 5 illustrates an exemplary implementation of the
process 200 for a VPN system implementing a Layer-2 VPN using
VPLS or VPW. While exemplary implementations of the process
200 are illustrated for a number of VPN technologies, those
20 skilled in the art, using the guidelines provided herein, may
modify the process 200 for various other VPN technologies
without departing from the spirit or the scope of the present
invention.

Referring now to Figure 3, an exemplary auto-
25 discovery process 300 for distributing VPN tunnel
configuration information in a Layer-3 PPVPN based on RFC
2547bis is illustrated in accordance with at least one
embodiment of the present invention. After determining the
relevant VCDI information (step 202, Figure 2), the process
30 300 initiates at step 302, wherein the VCDI information
associated with one or more VPN tunnels may be advertised to

the AD components of the PE routers (e.g., AD components 112, 114, Figure 1), as discussed above. As noted above, the VCDI information preferably is distributed as an extension of an auto-discovery protocol, such as BGP, DNS, or RADIUS. At step

5   304, the tunnel signalling component (e.g., tunnel signalling components 116, 118, Figure 1) at a PE router negotiates with the tunnelling mechanism at a corresponding PE router to establish and configure one or more VPN tunnels based at least in part on the supplied VCDI information. This configuration

10   may include, for example, negotiating QoS for the VPN tunnel, setting a minimum or maximum bandwidth for the VPN tunnel, specifying the tunnelling mechanism, and the like. Alternatively, in one embodiment, the tunnel signalling component may select a pre-existing VPN tunnel that complies

15   with some or all of the parameters set forth by in the VCDI information.

Upon creation and configuration of the VPN tunnel (or selection of a pre-existing tunnel), Virtual Routing Forwarding (VRF) tables may be generated at each PE router.

20   The generation of VRF tables is well known in the art. At step 306, these VRF tables then may be exported to the backbone using, for example, BGP and then distributed to the appropriate PE routers for use in routing VPN traffic through the established tunnel.

25   Referring now to Figure 4, an exemplary auto-discovery process 400 for distributing VPN tunnel configuration information in a Layer-3 VPN based on Virtual Routing is illustrated in accordance with at least one embodiment of the present invention. After determining the

30   relevant VCDI information (step 202, Figure 2), the process 400 initiates at step 402, wherein VPN IDs are associated with

14

the endpoints of the tunnel to be established/selected. At

this point, it typically is not necessary to advertise the VR

prefixes/addresses. At step 404, a list of the VPN IDs is

included with other VCDI information and this information may

5   be advertised to the AD components of the PE routers (e.g., AD

components 112, 114, Figure 1), as discussed above. For

Virtual Routing implementations, the VCDI information

preferably is distributed as an extension of a BGP

Multiprotocol Extension (BGP-MP). Other information

10   distribution protocols, such as DNS, RADIUS, and IP

multicasting may be utilized. At this point, it may be

appropriate to advertise the VR prefixes/addresses.

At step 406, the backbone Virtual Router receiving

the VCDI information may be adapted to establish and configure

15   one or more VPN tunnels based at least in part on the supplied

VCDI information. This configuration may include, for

example, negotiating QoS for the VPN tunnel, setting a minimum

or maximum bandwidth for the VPN tunnel, specifying the

tunnelling mechanism, and the like. Alternatively, in one

20   embodiment, the tunnel signalling component may select a pre-

existing VPN tunnel that complies with some or all of the

parameters set forth by in the VCDI information. At step 408,

the VPN topology information may be advertised in a manner

similar to the advertisement of the VCDI information at step

25   404.

Referring now to Figure 5, an exemplary auto-

discovery process 500 for distributing VPN tunnel

configuration information in a Layer-2 PPVPN based on VPLS or

VPW is illustrated in accordance with at least one embodiment

30   of the present invention. After determining the relevant VCDI

information (step 202, Figure 2), the process 500 initiates at

step 502, wherein the VCDI information associated with one or more VPN tunnels is advertised to the AD components of the PE routers (e.g., AD components 112, 114, Figure 1), as discussed above. At this point, it may be unnecessary to exchange

5 Layer-2 VPN services. As noted above, the VCDI information preferably is distributed as an extension of an auto-discovery protocol, such as BGP, DNS, or RADIUS.

At step 504, the tunnel signalling component (e.g., tunnel signalling components 116, 118, Figure 1) at a PE

10 router negotiates with the tunnelling mechanism at a corresponding router to establish and configure one or more VPN tunnels based at least in part on the supplied VCDI information. This configuration may include, for example, negotiating QoS for the VPN tunnel, setting a minimum or

15 maximum bandwidth for the VPN tunnel, specifying the tunnelling mechanism, and the like. Alternatively, in one embodiment, the tunnel signalling component may select a pre-existing VPN tunnel that complies with some or all of the parameters set forth by in the VCDI information.

20 Upon creation and configuration of the VPN tunnel (or selection of a pre-existing tunnel), Layer-2 VPN advertisements may be created at step 506 and distributed using the backbone BGP component (e.g., AD components 112, 114) at step 508.

25 At this point, it should be noted that implementing an auto-discovery VPN tunnel configuration process in accordance with the present invention as described above typically involves the processing of input data and the generation of output data to some extent. This input data

30 processing and output data generation may be implemented in hardware or software. For example, specific electronic

components may be employed in a node or similar or related circuitry for implementing an auto-discovery component and tunnel signalling component in accordance with the present invention as described above. Alternatively, one or more

5   processors operating in accordance with stored instructions may implement the functions associated with implementing an auto-discovery VPN tunnel configuration process in accordance with the present invention as described above. If such is the case, it is within the scope of the present invention that

10 such instructions may be stored on one or more processor readable media, or transmitted to one or more processors via one or more signals.

The present invention is not to be limited in scope by the specific embodiments described herein. Indeed, various

15 modifications of the present invention, in addition to those described herein, will be apparent to those of ordinary skill in the art from the foregoing description and accompanying drawings. Thus, such modifications are intended to fall within the scope of the following appended claims. Further,

20 although the present invention has been described herein in the context of a particular implementation in a particular environment for a particular purpose, those of ordinary skill in the art will recognize that its usefulness is not limited thereto and that the present invention can be beneficially

25 implemented in any number of environments for any number of purposes. Accordingly, the claims set forth below should be construed in view of the full breath and spirit of the present invention as disclosed herein.

17

CLAIMS

1.   A method for establishing a Virtual Private
Network (VPN) tunnel between a first provider edge (PE)
device and a second (PE) device of a Provider-Provisioned
5 VPN (PPVPN) comprising:

        advertising at least one tunnel-based parameter to
one or more PE devices over a network backbone using an
auto-discovery mechanism, the one or more PE devices
including at least one of the first and second PE devices;
10 and

        configuring a VPN tunnel between the first and
second PE devices based at least in part on the at least one
tunnel-based parameter.

2.   The method as in Claim 1, wherein the auto-
15 discovery mechanism includes one of a group consisting of: a
Border Gateway Protocol (BGP)-based mechanism; a Domain Name
Service (DNS)-based mechanism; and a Remote Authentication
Dial In User Service (RADIUS)-based mechanism.

3.   The method as in Claim 2, wherein the at least one
20 tunnel-based parameter is distributed to the one or more PE
devices as an extension of an auto-discovery protocol.

4.   The method as in Claim 1, wherein configuring the
VPN tunnel includes configuring the VPN tunnel using at
least one tunnel signalling mechanism.

25 5.   The method as in Claim 4, wherein the at least one
tunnel signalling mechanism includes one of a group
consisting of: a Resource Reservation Protocol (RSVP)-based
mechanism; a Resource Reservation Protocol-Traffic

18

Engineered (RSVP-TE)-based mechanism; a Label Distribution Protocol (LDP)-based mechanism; and a Constraint-based Routing LDP (CR-LDP) based mechanism.

6.   The method as in Claim 1, wherein the at least one
5   tunnel parameter includes one of a group consisting of: a type of tunnelling mechanism; at least one PE tunnel endpoint; at least one community route target; topology information; and at least one resource parameter.

7.   The method as in Claim 6, wherein the at least one
10 resource parameter includes one of a group consisting of: minimum bandwidth; maximum delay; committed burst size; committed rate; jitter; error; ownership; physical position and transport medium.

8.   A computer signal embodied in a carrier wave
15 readable by a computing system and encoding a computer program of instructions for executing a computer process for performing the method recited as in Claim 1.

9.   At least one processor readable carrier for storing a computer program of instructions configured to be
20 readable by at least one processor for instructing the at least one processor to execute a computer process for performing the method as recited in Claim 1.

10.   The method of Claim 1, wherein configuring the VPN tunnel includes selecting a pre-existing VPN tunnel, the
25 pre-existing VPN tunnel being compliant with the at least one tunnel parameter.

11.   In a Provider-Provisioned Virtual Private Network (PPVPN), a system comprising:

19

auto-discovery means for distributing at least one
Virtual Private Network (VPN) tunnel-based parameter to at
least a first and second provider edge (PE) devices; and

tunnel signalling means for configuring a VPN
5   tunnel over a network backbone between the first and second
PE devices based at least in part on the at least one
tunnel-based parameter.

12.   The system as in Claim 11, wherein the auto-
discovery means is adapted to distribute the at least one
10   tunnel-based parameter as an extension of at least one auto-
discovery protocol.

13.   The system as in Claim 12, wherein the auto-
discovery protocol comprises one of a group consisting of: a
Border Gateway Protocol (BGP)-based mechanism; a Domain Name
15   Service (DNS)-based mechanism; and a Remote Authentication
Dial In User Service (RADIUS)-based mechanism.

14.   The system as in Claim 11, wherein the tunnel
signalling means includes one of a group consisting of: a
Resource Reservation Protocol (RSVP)-based mechanism; a
20   Resource Reservation Protocol-Traffic Engineered (RSVP-TE)-
based mechanism; a Label Distribution Protocol (LDP)-based
mechanism; and a Constraint-based Routing LDP (CR-LDP) based
mechanism.

15.   The system as in Claim 11, wherein the at least
25   one tunnel parameter includes one of a group consisting of:
a type of tunnelling mechanism; at least one PE tunnel
endpoint; at least one community route target; topology
information; and at least one resource parameter.

20

16.   The system as in Claim 15, wherein the at least one resource parameter includes one of a group consisting of: minimum bandwidth; maximum delay; committed burst size; committed rate; jitter; error; ownership; physical position

5   and transport medium.

17.   In a distributed network, a Provider-Provisioned Virtual Private Network (PPVPN) system comprising:

a network backbone;

a first and second provider edge (PE) device, each

10 operably connected to the network backbone; and

an auto-discovery mechanism for distributing at least one VPN tunnel parameter to at least the first and second PE devices as an extension to an auto-discovery protocol.

15 18.   The system as in Claim 17, wherein the auto-discovery protocol comprises one of a group consisting of: a Border Gateway Protocol (BGP)-based mechanism; a Domain Name Service (DNS)-based mechanism; and a Remote Authentication Dial In User Service (RADIUS)-based mechanism.

20 19.   The system as in Claim 17, further comprising a tunnel signalling mechanism adapted to configure a VPN tunnel between the first PE device and the second PE device based at least in part on the at least one tunnel-based parameter.

25 20.   The system as in Claim 19, wherein the tunnel signalling mechanism includes one of a group consisting of: a Resource Reservation Protocol (RSVP)-based mechanism; a Resource Reservation Protocol-Traffic Engineered (RSVP-TE)-

21

based mechanism; a Label Distribution Protocol (LDP)-based mechanism; and a Constraint-based Routing LDP (CR-LDP) based mechanism.

21.   The system as in Claim 17, wherein the at least one tunnel parameter includes one of a group consisting of: a type of tunnelling mechanism; at least one PE tunnel endpoint; at least one community route target; topology information; and at least one resource parameter.

1/5

Fig. 1

```
┌─────────────────────────────────┐
│   Determine VPN Capability      │
│  Discovery Information (VCDI)   │
│              202                │
└─────────────────────────────────┘
                │
                │                          200
                ▼
┌─────────────────────────────────┐
│      Advertise VCDI to PEs      │
│              204                │
└─────────────────────────────────┘
                │
                ▼
┌─────────────────────────────────┐
│ Construct tunnel between near PE │
│   and distant PE using VCDI     │
│              206                │
└─────────────────────────────────┘
```

Fig. 2

VPN Capability Discovery for Layer-3 VPNs using 2547bis

```
┌──────────────────────────────────────┐
│         Advertise VCDI to PEs         │
│                 302                   │
└──────────────────────────────────────┘
                    │
                    ▼                         300
┌──────────────────────────────────────┐
│     Negotiate QoS by creating PE-PE   │
│               tunnel(s)               │
│                 304                   │
└──────────────────────────────────────┘
                    │
                    ▼
┌──────────────────────────────────────┐
│    Export VRF tables to backbone for  │
│              distribution             │
│                 306                   │
└──────────────────────────────────────┘
```

Fig. 3

VPN Capability Discovery for Layer-3 VPNs using Virtual Routing

```
┌─────────────────────────────────┐
│  Associate VPN IDs with tunnel  │
│           endpoints             │
│              402                │
└─────────────────────────────────┘
                │
                ▼                          400
┌─────────────────────────────────┐
│  Advertise VCDI using BGP-MP    │
│              404                │
└─────────────────────────────────┘
                │
                ▼
┌─────────────────────────────────┐
│  Create PE-PE tunnel by backbone │
│              VR                 │
│              406                │
└─────────────────────────────────┘
                │
                ▼
┌─────────────────────────────────┐
│  Advertise topology information  │
│              408                │
└─────────────────────────────────┘
```
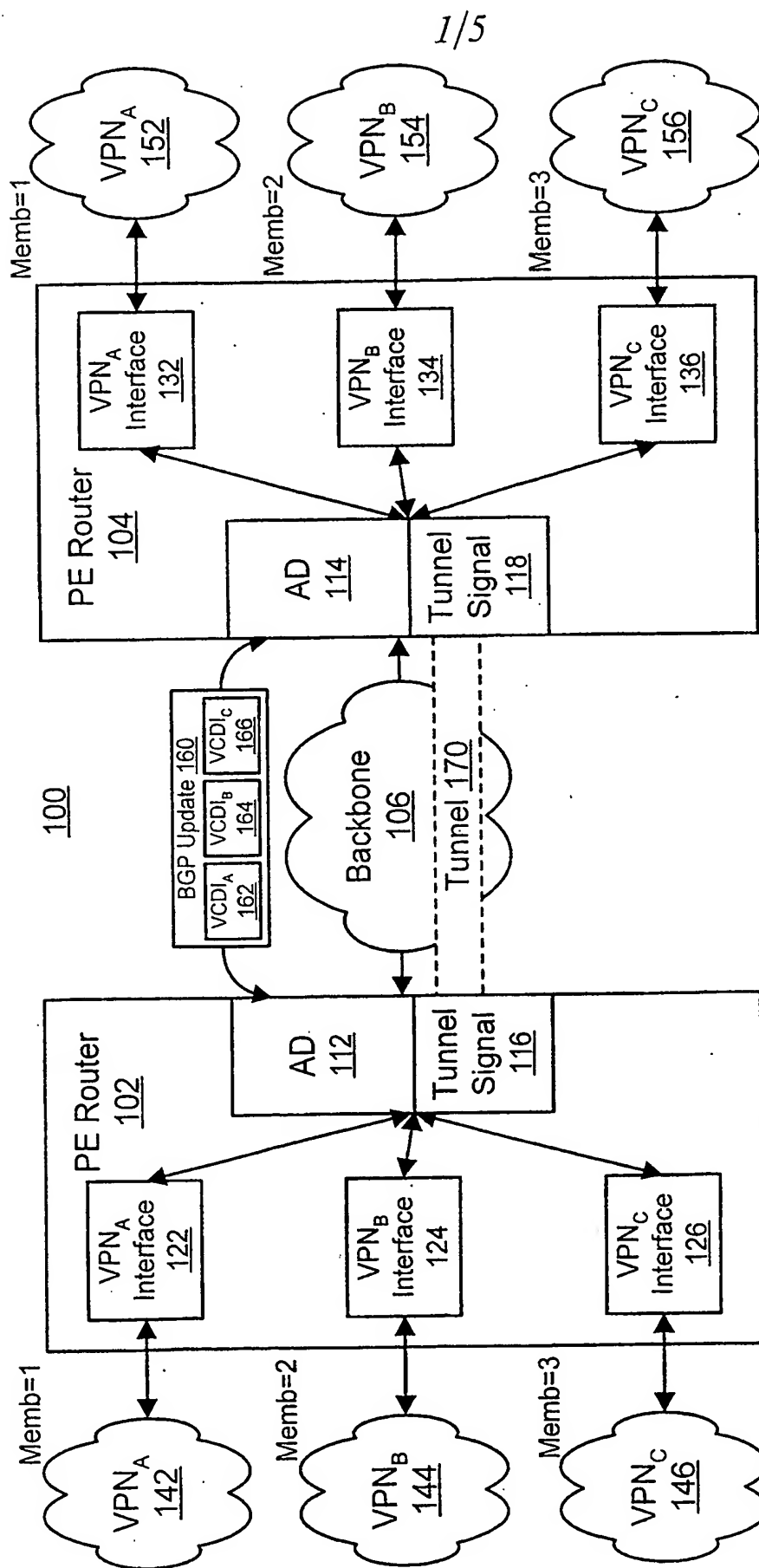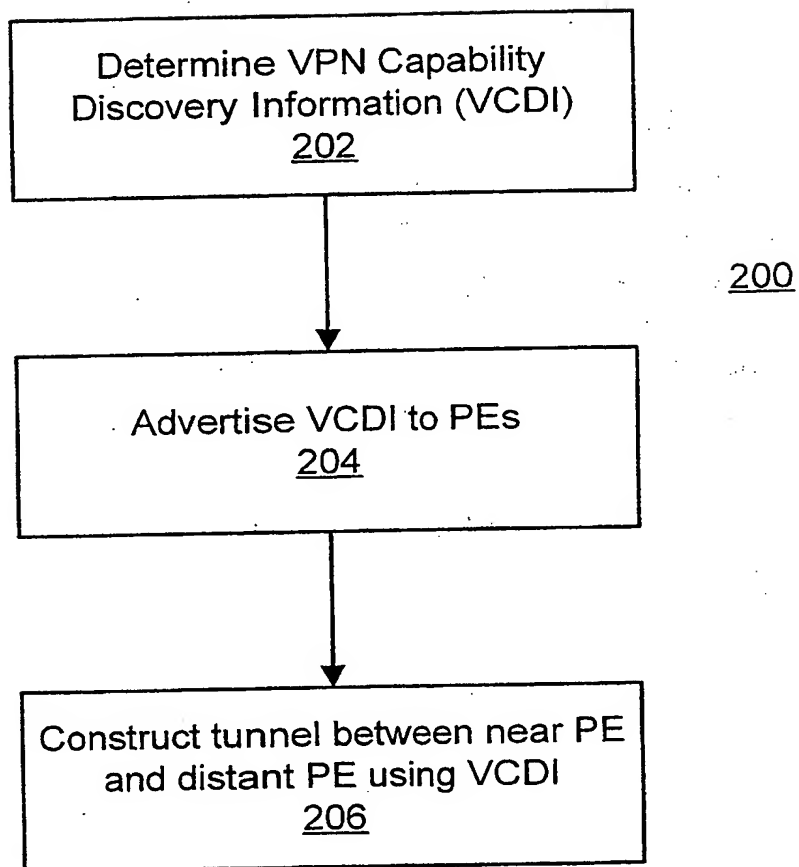
FIG. 4

5/5
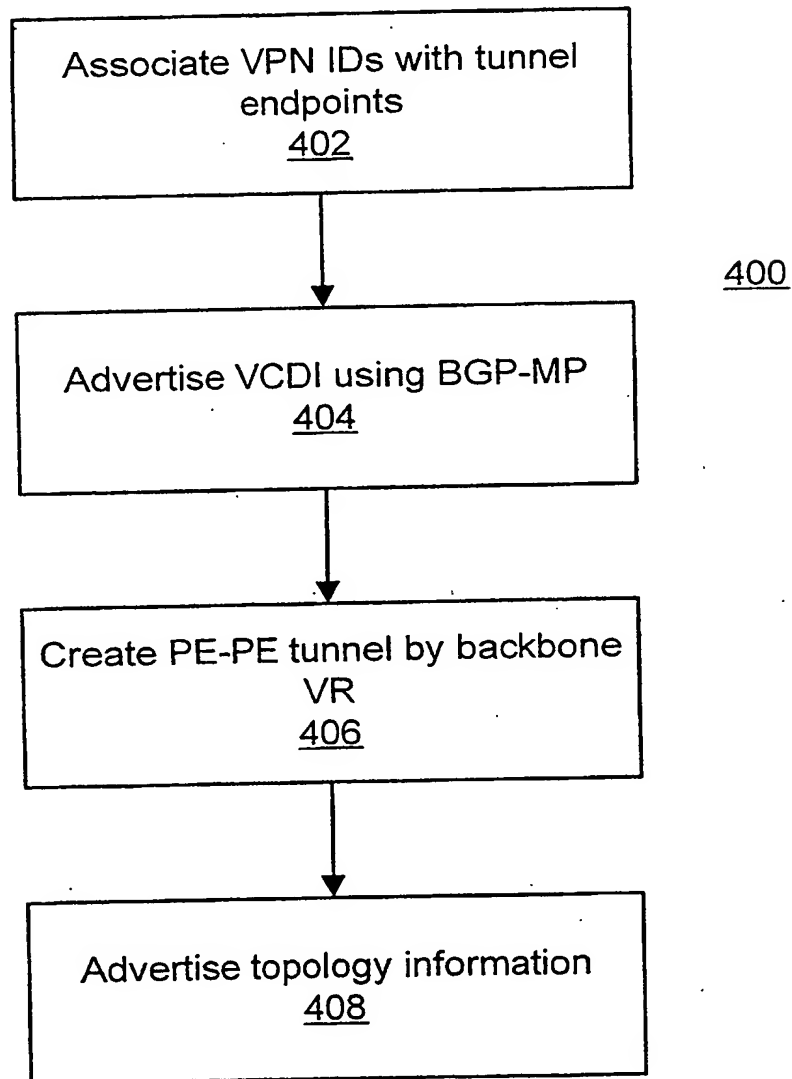
VPN Capability Discovery for Layer-2 VPNs
using VPLS or VPW
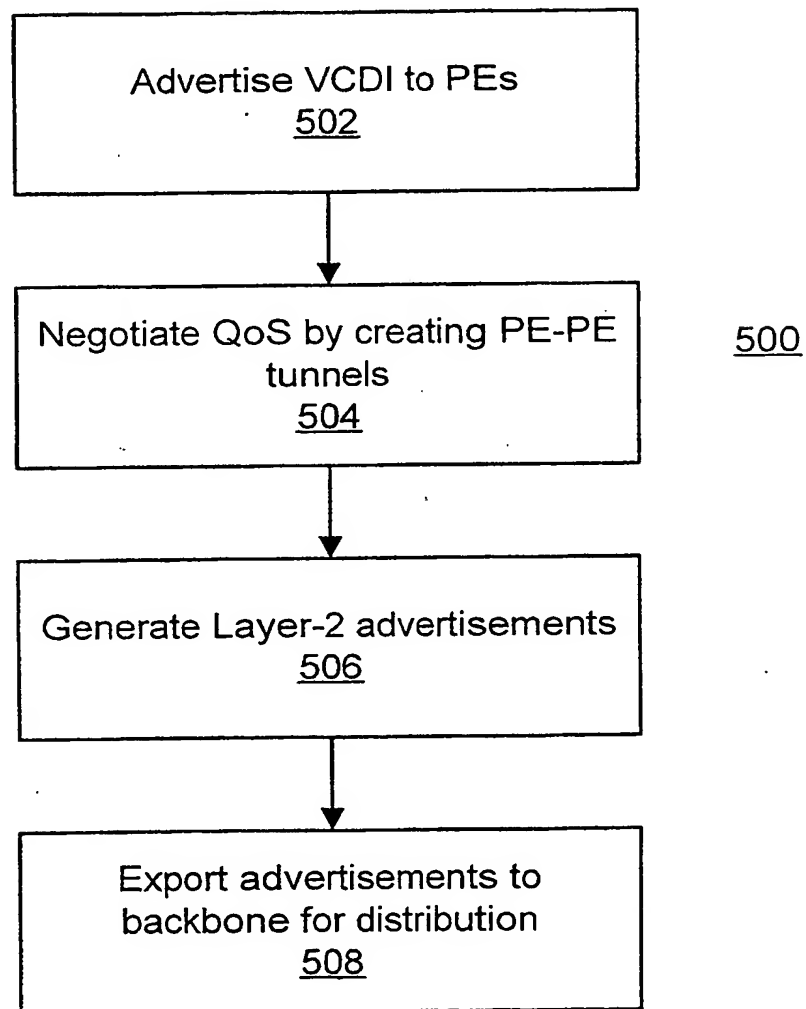
```
┌─────────────────────────────────┐
│     Advertise VCDI to PEs        │
│             502                  │
└─────────────────────────────────┘
                │
                ▼
┌─────────────────────────────────┐
│  Negotiate QoS by creating PE-PE │        500
│            tunnels               │
│             504                  │
└─────────────────────────────────┘
                │
                ▼
┌─────────────────────────────────┐
│  Generate Layer-2 advertisements │
│             506                  │
└─────────────────────────────────┘
                │
                ▼
┌─────────────────────────────────┐
│    Export advertisements to      │
│   backbone for distribution      │
│             508                  │
└─────────────────────────────────┘
```

Fig. 5

INTERNATIONAL SEARCH REPORT

A. CLASSIFICATION OF SUBJECT MATTER

IPC 7 H04L12/46 H04L12/24

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC 7 H04L H04Q

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category°	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 6 079 020 A (LIU QUENTIN C) 20 June 2000 (2000-06-20) column 2, line 15 -column 3, line 21 abstract; claims 1,2 ---	1-21
X	US 6 085 238 A (OHNO MASAMI ET AL) 4 July 2000 (2000-07-04) column 1, line 14 - line 24 column 6, line 56 -column 7, line 27 column 10, line 8 - line 33 column 10, line 62 -column 11, line 17 abstract ---	1-21
P,X	US 6 473 863 B1 (SHIEH JOHNNY MENG-HAN ET AL) 29 October 2002 (2002-10-29) column 2, line 1 - line 30 abstract; claim 1 -----	1-21

☐ Further documents are listed in the continuation of box C.   ☒ Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
15 May 2003	03. 06. 2003

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	RALF BOSTRÖM/JA A

Form PCT/ISA/210 (second sheet) (July 1992)

Patent document cited in search report		Publication date	Patent family member(s)		Publication date
US 6079020	A	20-06-2000	NONE		
US 6085238	A	04-07-2000	JP	3124926 B2	15-01-2001
			JP	9289521 A	04-11-1997
			JP	9288627 A	04-11-1997
			JP	10190716 A	21-07-1998
			JP	10190715 A	21-07-1998
			JP	3201731 B2	27-08-2001
			JP	10224391 A	21-08-1998
US 6473863	B1	29-10-2002	DE	10052312 A1	08-11-2001

Form PCT/ISA/210 (patent family annex) (July 1992)